CLAIMS

1. A method, comprising:

associating a digital signature with a web page; and

delivering the web page to an electronic device capable of authenticating the digital signature and executing at least a portion of the web page after the digital signature is authenticated.

2. The method as recited in claim 1, wherein the associating further comprises attaching the digital signature to the web page.

3. The method as recited in claim 1, further comprising:

determining if the web page includes code to invoke a control object; and

deriving the digital signature and associating the digital signature with the web page only if the web page includes code to invoke a control object.

4. The method as recited in claim 1, wherein the web page includes a confirmation module that is used by the electronic device to authenticate the digital signature.

5. The method as recited in claim 1, wherein the web page contains script that, when executed, invokes executable code that is executed on the electronic device executing the web page.

6. The method as recited in claim 1, wherein the web page is generated in an active server page (ASP) environment.

7.   A method, comprising:

receiving a web page from a server, the web page containing executable script that, when executed, invokes a control object, the web page having a segment that uniquely identifies a source of the web page;

authenticating the source of the web page; and

displaying the web page and invoking the control object if the web page is authenticated.

8.   The method as recited in claim 7, further comprising:

determining if the source of the web page is authorized to invoke the control object; and

displaying the web page only if the source of the web page is authorized to invoke the control object.

9.   The method as recited in claim 7, wherein the authenticating further comprises authenticating the source of the web page to identify the source of the web page.

10.   The method as recited in claim 7, further comprising:

designating one or more authorized sources from which a web page that invokes a control object may be received; and

executing script contained in the web page only if authenticating the source of the web page indicates that the web page was received from an authorized source.

11. A system, comprising:

a page generator to generate a web page;

a digital signature module configured to derive a digital signature from the web page and attach the digital signature to the web page; and

a page delivery module to deliver the signed web page to an electronic device.

12. The system as recited in claim 11, the digital signature module being further configured to determine whether the web page contains script to invoke executable code, and to apply a digital signature to the web page only if the web page contains script to invoke executable code.

13. The system as recited in claim 11, further comprising:

a control object in the web page;

script in the web page that invokes the control object; and

wherein the control object includes executable instructions that are executable on the electronic device that receives the web page.

14. The system as recited in claim 11, further comprising:

a confirmation module configured to authenticate the digital signature.

15. The system as recited in claim 14, wherein the confirmation module is included in the control object.

16. The system as recited in claim 14, wherein the confirmation module is included in a browser of the electronic device.

17. A system, comprising:

a web browser configured to access a web page having a digital signature;

a processor configured to execute script contained in the web page;

an executable control object that may be invoked by the script in the web page and is executable on the processor;

a confirmation module configured to authenticate the digital signature; and

wherein the confirmation module is called when the control object is invoked by the script, the control object executing only if the confirmation module authenticates the digital signature.

18. The system as recited in claim 17, wherein the confirmation module is called by the control object.

19. The system as recited in claim 17, wherein the confirmation module is included in the control object.

20. The system as recited in claim 17, wherein the confirmation module is included in the web browser.

21.   The system as recited in claim 17, wherein the confirmation module is further configured to determine if the web page comes from a source that is authorized to invoke the control object and the control object is invoked only if the source of the web page is authorized to invoke the control object.

22.   The system as recited in claim 17, wherein the confirmation module is called by the web page prior to the web page invoking the control object.

23.   The system as recited in claim 17, wherein the digital signature module is not invoked if the web page does not have a digital signature.

24.   A web page contained on a computer-readable medium, comprising:
    computer-executable script that, when executed on a computing device, invokes an executable control object on the computing device; and
    a digital signature uniquely identifying an author of the web page.

25.   The web page as recited in claim 24, wherein the digital signature is appended to the contents of the web page.

26.   The web page as recited in claim 24, further comprising the executable control object.

27. A web browser contained on a computer-readable medium of a client computer, comprising computer-executable instructions that, when executed by the client computer, perform the following:

determining if a web page contains instructions to invoke a control object;

authenticating the web page using a digital signature; and

invoking the control object if the source of the web page is authenticated.

28. The web browser as recited in claim 27, further comprising:

determining if the web page contains executable script to invoke a control object; and

wherein the authenticating the web page further comprises authenticating the web page only if the web page contains executable script to invoke a control object.

29. The web browser as recited in claim 27, further comprising:

determining if the web page contains a digital signature; and

wherein the authenticating the web page further comprises authenticating the web page only if the web page contains a digital signature.

30. The web browser as recited in claim 27, wherein the control object is not invoked if the web page does not include a digital signature.

31. The web browser as recited in claim 27, further comprising instructions to determine if an authenticated web page comes from a source that is authorized to invoke the control object.

32. A control object stored in a computer-readable medium, comprising computer-executable instructions that, when executed on a computer, perform the following:

authenticating a web page that invokes the control object; and

executing a data-handling task on the computer if the web page is determined to be authentic.

33. The control object as recited in claim 32, wherein the web page is authenticated utilizing a digital signature attached to the web page.

34. The control object as recited in claim 32, further comprising instructions to determine if a source of the web page is authorized to invoke the data-handling task prior to executing the data-handling task.

35. A modulated data signal having data fields encoded thereon transmitted over a communication channel, comprising:

a first data field containing data representing a web page; and

a second data field containing data representing a digital signature derived from the web page represented by the first data field.